

REMARKS

I. Introduction

Claims 1-58 are pending in the present application. In a June 19, 2006, Office Action (herein "Office Action"), Claims 1-13, 24-29, 31-41, and 45-58 were rejected under 35 U.S.C. § 101 as not being statutory. Claims 1, 2, 14, 18-22, 31-36, 42, 43, 45-50, and 56-58 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,023,223 to Baxter et al. (herein "Baxter"). Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Baxter in view of U.S. Patent No. 6,714,977 to Fowler (herein "Fowler"). The Office Action rejected Claims 8, 23, 26, and 44 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, and in further view of in view of U.S. Patent No. U.S. Patent No. 6,429,893 to Xin (herein "Xin"). The Office Action rejected Claims 27-30 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, Xin, and further in view of U.S. Patent No. 6,219,439 to Burger (herein "Burger"). Applicants respectfully submit that the rejected claims of the present application are not anticipated nor obvious over the cited references, alone or in combination, because the cited references fail to teach or suggest processing monitoring device data in accordance with a set of monitoring device rules.

Pursuant to 37 C.F.R. § 1.111, and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to presenting the reasons why applicants believe that the pending claims are in condition for allowance, a brief summary of the present invention, as well as the cited references are presented. However, it should be appreciated that the following summaries are presented solely to assist the Examiner in recognizing the differences between the pending claims and the cited reference, and should not be construed as limiting upon the present invention.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSTM, L.C.
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

A. Summary of the Present Application

The present application is generally directed toward a system and method of implementing a configurable security monitoring system for a plurality of remote monitoring sites. In accordance with an illustrative embodiment, a method is provided that obtains monitoring device data from the at least one monitoring device and one or more rules. The one or more rules establish a threshold for the monitoring device data based on input received from the monitoring device. The input is processed according to the monitoring rules to determine whether a rule violation has occurred. When a rule violation is identified, an authorized user may be notified of the violation.

B. Summary of Baxter et al. (U.S. Patent No. 6,023,223)

Baxter is purportedly directed at a system and method for early warning detection and notification of environmental conditions. In this regard, Baxter uses a plurality of remotely located environmental sensors having a communication uplink to one or more Earth-orbiting satellites or other wireless transmission means. The environmental sensors periodically upload environmental condition data to a satellite. Then, the satellite downloads the condition data to the database server where an interface provides access to the condition data through a network such as the Internet. The environmental conditions monitored by the system in Baxter include hydrocarbon concentrations, water temperature, wind speed, plate tectonics, atmospheric pressure, toxin concentrations, and the like. Additional applications may include tracking of animal migrations and densities, deforestation, polar ice cap activity, red tide, and other geological, biological, atmospheric, and oceanic conditions.

C. Summary of Fowler et al. (U.S. Patent No. 6,714,977)

Fowler is purportedly directed toward a system and method for monitoring an enclosed space over a communication network. Generally described, Fowler teaches the utilization of

various low cost, independent monitoring components (e.g., "bots"), that monitor and report various conditions associated with a monitored space. Each bot is specifically configured to monitor specific parameters, such as a climate bot, a video climate bot, a net bot, etc. In turn, each bot processes raw monitored data and provides processed data to a user over a communication network. Thus, Fowler is directed toward a de-centralized monitoring environment. Fowler, however fails to teach or suggest a centralized server component that obtains monitoring device data from monitoring devices at geographically distinct sites and processes the data according to various monitoring device rules. Fowler further fails to teach or suggest characterizing the monitoring device data as asset, resource or event data.

II. Claim Rejections Under 35 U.S.C. § 101 and 35 U.S.C. § 112

The Office Action rejected Claims 1-58 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. Moreover, the Office Action rejected Claims 1-13, 24-29, 31-41, and 45-58 under 35 U.S.C. § 101 as not being statutory subject matter. For both rejections, the Office Action objected to the use of the limitation that recited "an output may include no output." For each of the pending claims in the application, this recitation has been removed to overcome these objections.

III. The Claims Distinguished

A. Claim Rejections Under 35 U.S.C. § 102

The Office Action rejected Claims 1, 2, 14, 18-22, 31-36, 42, 43, 45-50, and 56-58 under 35 U.S.C. § 102(b) as being anticipated by Baxter. The Office Action asserts that Baxter discloses each of the elements of applicants' claims. Applicants respectfully disagree. As described in more detail below, the cited reference fails to disclose or suggest certain elements of the independent and dependent claims.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

1. Claim 1

Claim 1 recites the following:

1. In an integrated information system including a central server in communication with two or more geographically distinct sites, a method for processing monitoring device data, the method comprising:

obtaining monitoring device data from the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously;

obtaining one or more monitoring rules corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation;

processing the monitoring device data at the central server according to the monitoring rules to determine whether a rule violation occurred wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices; and

generating an output corresponding to the processing of the monitoring device data, wherein the output indicates whether a rule violation occurred.

As mentioned briefly above, the present application is directed toward a system and method of implementing a configurable security monitoring system for a plurality of remote monitoring sites. In this regard, monitoring device data is obtained continuously to determine whether a rule violation has occurred. More specifically, Claim 1 recites "obtaining monitoring device data . . . wherein the monitoring device data is obtained continuously." For example, as recited in the present application, "the central server 56 may poll individual devices for an input." Present application at page 13. In the context of a security monitoring system, continuously obtaining monitoring device data by "polling" individual devices is advantageous as the immediacy of notifying an authorized user is important. For example, aspects of the present

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

invention may be used to determine whether an emergency is occurring on a premises being monitored. If an emergency is occurring, the appropriate personnel may be notified in a timely manner.

In contrast to the claims of the present invention, Baxter is directed to an Internet-based global network for retrieving, storing, and displaying real time environmental data. In this regard, Baxter describes a computer system comprised of a plurality of remotely located environmental sensors having a communications uplink to a communication relay, a downlink interface from the satellite to a database server having one or more data tables holding environmental data. In this regard, the environmental "sensors *periodically* upload environmental condition data to the satellite, the satellite downloads the condition data to the database server, the communication interface provides access to the condition data through the Internet. [Emphasis added]." Baxter at Col. 3, lines 14-19.

While periodically uploading environmental condition data to a satellite may have benefits when environmental conditions are being monitored by satellite, the system disclosed in Baxter could not be applied to obtaining security data. More specifically, by periodically uploading data, the Baxter system does not satisfy the time sensitive requirements of a security monitoring system. In contrast to the system disclosed in Baxter, Claim 1 of the present invention recites obtaining monitoring device data continuously. For example, the monitoring device data may be obtained continuously when a central server polls the monitoring device data from a remotely located monitoring device.

As distinctly defined in Claim 1 and described in the specification, applicants' claimed method is a combination that includes "obtaining one or more monitoring rules . . . wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation, and wherein a rule violation identifies a combination of thresholds for each of the two

monitoring devices." In this regard, a user of the present invention has the ability to configure the security monitoring system to match the attributes of a premises being monitored. For example, a rule may define thresholds for each of the two monitoring devices that is required to generate a rule violation. If the thresholds for each of the monitoring devices are not satisfied, then a rule violation has not occurred. These limitations recited in Claim 1 are reflected in examples provided in the present application. As stated in the present application, "a rule corresponding to a glass break detector may indicate that a motion detector signal must be detected before the rule is violated." Present application at page 14. The security monitoring system as recited in Claim 1 provides a highly configurable system in which a combination of thresholds from monitoring devices define a rule violation. Among other things, this highly configurable security system allows users to determine how "sensitive" the security system will be in identifying a rule violator. As distinctly recited in Claim 1, rules may be defined in which a combination of thresholds for each monitoring device are required to generate a rule violation.

In contrast to Claim 1, Baxter is directed toward a system and method for periodically obtaining environmental data. To determine whether an authorized user should be notified of an event in the Baxter system, a combination of thresholds in a rule is not analyzed. While the system disclosed in Baxter obtains different types of environmental data, this data is not used to determine whether additional actions related to the collected data will be performed. Instead, the data is used to correlate different types of environmental conditions. As stated in Baxter:

Data retrieved at a specific date, time, latitude, and longitude for ozone concentration may be matched against the atmospheric temperature at that same location and time. Using the reference fields, researchers are able to correlating [sic] different environment conditions and establish theoretic models of environmental interrelationships from empirical data.

Baxter at Col. 7, lines 31-38. As this example illustrates, the Baxter system may be used to obtain data using remotely located environmental sensors. In this regard, hydrocarbon

concentrations, water temperature, wind speed, plate tectonics, and the like may be analyzed. However, the system as disclosed in Baxter does not teach obtaining one or more rules that establish the thresholds of monitoring device data that define a rule violation, wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices. Instead, the Baxter system discloses matching different types of environmental data from a relational database. Through this matching, researchers may correlate the different environmental conditions so that theoretic models of environmental interrelationships may be established. In contrast to the present invention, Baxter does not define rules in which thresholds of monitoring device data from two monitoring devices are used to establish a rule violation.

As described above, Baxter fails to teach or suggest an integrated information system in which monitoring device data is obtained continuously. Moreover, Baxter fails to teach or suggest obtaining one or more monitoring rules wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation, and wherein a rule violation identifies a combination of thresholds for the monitoring devices. Instead, Baxter is clearly directed toward an early warning detection and notification network regarding environmental conditions. Events that require notification of an authorized user are not defined in rules that identify multiple thresholds when determining whether a rule violation has occurred. When determining whether an oil spill or other environmental event occurred, the Baxter system merely needs to determine whether a threshold level of hydrocarbons have been identified from sensors in the ocean. Thus, Baxter fails to teach or suggest "obtaining one or more monitoring rules . . . wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation, and wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices," as recited in Claim 1. Additionally, Baxter fails to teach or suggest "continuously obtaining monitoring device data from two monitoring devices." Since

Baxter fails to teach each limitation recited in Claim 1, applicants respectfully request a withdrawal of the 35 U.S.C. § 102(e) rejection of Claim 1.

2. Claims 2, 14, 18-22, and 31-33

Claims 2, 14, 18-22, 31-33 depend on independent Claim 1. As discussed above, Baxter fails to teach or suggest processing monitoring device data as defined in Claim 1. Accordingly, for the above-mentioned reasons, Claims 2, 14, 18-22, and 31-33 are also allowable over Baxter. Additionally, Claims 2, 14, 18-22, and 31-33 are not anticipated by Baxter, as claimed in the Office Action, for additional reasons discussed below.

Claim 2 includes the limitation of determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred. As described above, Baxter is directed at collecting environmental data to determine whether an environmental emergency has occurred. In contrast, aspects of the present invention are directed to an integrated information system for obtaining security information when determining whether an unauthorized access of a premises has occurred. Applicants respectfully assert that Baxter in no way teaches an integrated information security system as recited in Claim 2.

Claim 14 adds the additional limitation of generating a communication to one or more designated users, wherein generating the communication includes identifying a hierarchy that prioritizes the communication to the one or more designated users. The Office Action asserts that Baxter teaches generating a communication to one or more designated users. Office Action at page 5. Applicants agree that the Baxter system is configured to communicate with designated users when an abnormal condition is identified, such as abnormal environmental conditions. In this instance, a communication that is widely distributed may be created and transmitted. However, the Baxter system does not include identifying a hierarchy that prioritizes the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

communication to the one or more designated users, as disclosed in the present application. In this regard, aspects of the present invention are able to distribute information to the appropriate user. If the appropriate user is not readily available by telephone, then the user may be contacted using other communication means, such as fax, pager, and the like. Accordingly, Baxter fails to teach or suggest the additional element recited in Claim 14. Thus, applicants assert that this claim is also allowable for this additional reason.

Claim 19 has the additional recitation of "generating an output corresponding to the processing of the monitoring device data includes initiating an action at a geographically distinct site where the monitoring data was obtained." As mentioned previously, the Baxter system is directed at collecting environmental data from sensors that may be remotely located. In contrast, aspects of the present invention are directed at securing premises from unauthorized access. In this regard, processing performed by the present invention may determine that an unauthorized access has occurred in response to a rule violation. In this instance, additional actions that occur at a geographic site where the monitoring data was obtained may be performed. For example, aspects of the present invention may cause an audible alarm to be sounded, thereby giving audible notice that an unauthorized access is occurring. Applicants respectfully assert that Baxter in no way teaches initiating an action at a geographic site where monitoring device data was obtained. Accordingly, applicants further assert that Baxter fails to teach or suggest the additional limitation of Claim 19.

3. Claims 34 and 48

Claim 34 recites the following:

34. A system for implementing an integrated information system, the system comprising:

one or more monitoring devices corresponding to two or more geographically distinct sites organized according to geographic criteria and operable to continuously transmit monitoring device data;

a central processing server, the central processing server operable to continuously obtain the monitoring device data from at least one monitoring device at each of the two or more geographically distinct sites;

wherein the central processing server processes the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria, wherein the central processing server generates an output corresponding to the processing, wherein the output reflects the results of processing the monitoring device data according to the rules; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

Claim 48 recites the following:

48. A system for implementing an integrated information system, the system comprising:

one or more monitoring devices operable to continuously transmit monitoring device data from two or more geographically distinct sites organized according to geographic criteria;

central processing means for obtaining the monitoring device data from the one or more monitoring devices, processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria and generating outputs corresponding to the processing, the output reflects the results of processing the monitoring device data according to the rules; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

Each of the Claims 34 and 48 includes the limitations of "processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices" and "wherein the monitoring device rules identify a combination of

thresholds for the monitoring device data that define a rule violation." As described previously, a user of the present invention has the ability to configure the security monitoring system to match the attributes of a premises being monitored. For example, a rule may define thresholds that is required to generate a rule violation. However, Baxter is clearly directed toward an early warning detection and notification network regarding environmental conditions. Events that require notification of an authorized user are not defined in rules that identify multiple thresholds. In this regard Baxter fails to teach or suggest "processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices" and "wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation." Since Baxter fails to teach each limitation recited in Claims 34 and 48, applicants respectfully request a withdrawal of the 35 U.S.C. § 102(e) rejection of these claims.

B. Rejection of Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 Under 35 U.S.C. § 103(a)

The Office Action rejected Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 under 35 U.S.C. § 103 as being unpatentable over Baxter in view of Fowler. The Office Action asserts that Baxter and Fowler disclose each of the elements of applicants' claims and that it would have been obvious to a person of ordinary skill in the art to combine the teachings of the cited references at the time this invention was made. Applicants respectfully disagree. As described in more detail below, the cited references fail to disclose or suggest elements of these dependent claims. Moreover, applicants submit that it would not have been obvious to combine the teachings of the cited references at the time the invention was made.

Claims 3-7, 9-13, 15-17, 24, and 25 depend from independent Claim 1. Similarly, Claims 37-41 and 51-55 depend from independent claims 34 and 48, respectively. As discussed above, Baxter fails to teach or suggest obtaining one or more monitoring rules, wherein the one or more

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

rules establish the thresholds of monitoring device data that define a rule violation, and wherein a rule violation identifies a combination of thresholds for each of the monitoring devices. Accordingly, for the above-mentioned reasons, Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 are allowable over Baxter alone, or in combination, with Fowler. Additionally, Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 further add to the non-obviousness of applicants' invention, some of the details of which are discussed below.

Claim 3, 37, and 51 add the additional limitation of "wherein the one or more monitoring devices are characterized as asset data, resource data, or event data, wherein asset data includes data from an identifiable object that is not capable of independent action, wherein resource data includes data from an object capable of independent action, and wherein event data includes data from a device having a defined state." The Office Action asserts that Baxter teaches obtaining asset data and resource data. Office Action at page 7. Then, the Office Action acknowledges that Baxter does not disclose obtaining sensor data from a device having a defined state. However, the Office Action asserts that Fowler discloses another integrated information system for processing monitoring device data which discloses obtaining event data from a device having a defined state. In asserting that Baxter discloses characterizing monitoring device data as asset data or resource data, the Office Action states "the data must be characterized since thresholds pertaining to a temperature alarm setting would not be useful for an oil detection buoy data." Office Action at page 6. Applicants respectfully submit that the Office Action is reading into the disclosure of Baxter the limitation of characterizing the monitoring device data as asset data or resource data. While the Baxter system may characterize data in certain ways by determining whether the data relates to temperature levels, hydrocarbon levels, and the like, applicants are unable to find any characterization performed by Baxter that differentiates the data based on the type of monitoring device that the data was collected. Accordingly, the cited references fail to

teach or suggest the additional elements recited in Claims 3, 37, and 51. Thus, applicants assert that these claims are also allowable for these additional reasons.

Claim 7 adds the additional limitation of "wherein the device rules establish a state threshold for a rule violation and wherein processing the monitoring device data according to the device rules includes determining whether the monitoring device data indicates a particular state." The Office Action asserts that Fowler discloses that the device rules establish a state threshold for a rule violation and determining whether the monitoring device data indicates a particular state. In support of that proposition, the Office Action refers to Figure 17 of Fowler that illustrates the triggering of a smoke alarm. Applicants respectfully submit that rules which establish a state threshold for a rule violation is not equivalent to using an off-the-shelf smoke alarm to indicate a particular state. Accordingly, the cited references fail to teach or suggest the additional element recited in Claim 7.

In regard to Claims 15-17, the Office Action took "Official Notice" that both the concept and advantages of maintaining a schedule of preferred notification methods based on a time of day and preferred notification methods for each designated user is well known and expected in the art. Applicants respectfully disagree. As distinctly claimed in Claims 15-17, "a schedule of preferred notification methods" is used to determine how an authorized user will be notified of a rule violation. While Fowler does disclose notifying an authorized user, Fowler does not disclose a method for selecting the appropriate notification method that depends on a variable such as the time of day. The Office Action incorrectly equates contacting an authorized user with processing performed to identify a schedule of preferred notification methods. Then, the Office Action inappropriately takes Official Notice that the concept and advantages of providing a schedule of preferred notification methods is well known and expected in the art.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

C. Rejection of Claims 8, 23, 26, and 44 Under 35 U.S.C. § 103(a)

The Office Action rejected Claims 8, 23, 26, and 44 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, and in further view of in view of U.S. Patent No. U.S. Patent No. 6,429,893 to Xin (herein "Xin"). The Office Action asserts that Baxter, Fowler, and Xin disclose each of the elements of applicants' claims and that it would have been obvious to a person of ordinary skill in the art to combine the teachings of the cited references at the time this invention was made. Applicants respectfully disagree. As described in more detail below, the cited references fail to disclose or suggest elements of these dependent claims. Moreover, applicants submit that it would not have been obvious to combine the teachings of the cited references at the time the invention was made.

Claim 8, adds to the non-obviousness of applicants invention the limitation of "wherein the monitoring device data is motion detection data and wherein the device rule threshold is the detection of motion." The Office Action states that "it is an inherent feature to any motion detector that there must be a lower limit threshold to flag an alert (such as a person walking by, not a piece of paper blowing in the wind)." Office action at page 12. However, the limitation as recited in Claim 8 does not refer to the inherent abilities of a motion detector. Instead, the limitation recited in Claim 8 refers to processing the data produced from the motion detector in accordance with a rule. For example, a rule may be established in which a rule violation does not occur until a motion detector detects motion for a specified period of time (e.g. 10 seconds). This ability as reflected in the additional limitation recited in Claim 8 does not appear in any of the cited references.

D. Rejection of Claims 27-30 Under 35 U.S.C. § 103(a)

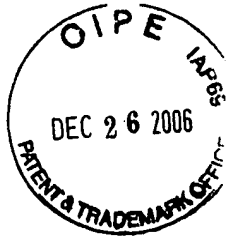
The Office Action rejected Claims 27-30 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, Xin, and further in view of U.S. Patent No. 6,219,439 to Burger (herein

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

"Burger"). Claims 27-30 depend from independent Claim 1. As discussed above, Baxter fails to teach or suggest obtaining one or more monitoring rules, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation, and wherein a rule violation identifies a combination of thresholds for each of the monitoring devices. Accordingly, for the above-mentioned reasons, Claims 27-30 are allowable over Baxter alone, or in combination, with Fowler, Xin, and Burger. Additionally, Claims 27-30 further add to the non-obviousness of applicants' invention, some of the details of which are discussed below.

Claims 28 adds to the nonobviousness of applicants invention the limitation of using the monitoring device to identify the location of the individuals within the premises. Applicants are unable to find any teaching in the cited references that describe identifying the location of an individual within a premises. Applicants agree that Burger teaches using a "smart card" to verify an individual's identity. However, Burger does not teach identifying the location of an individual within a premises. The Office Action incorrectly equates verifying an individual identity with determining the location of a user within a premises.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100



CONCLUSION

In view of the amendments and remarks above, applicant respectfully submits that the pending claims are in condition for allowance. Reconsideration and reexamination of the application, as amended, and allowance of the claims at an early date are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first-class mail with postage thereon fully prepaid and addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: December 19, 2006

CJF:jljg

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100